United States
Department of Agriculture

Office of the Chief Information Officer

DN 3300-012

Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Networks in Unlicensed Frequencies

Commercial Wireless Technologies in USDA -
Unclassified Security Requirements for Wireless Networks in Unlicensed Frequencies

TABLE OF CONTENTS

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

# DEPARTMENTAL NOTICE	**Number:** 3300-012
SUBJECT: Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Networks in Unlicensed Frequencies	**DATE:** April 20, 2005
	OPI: Office of the Chief Information Officer, Telecommunications Policy and Planning Division
CODIFICATION/EXPIRATION: This Notice will expire one year from the date it is signed, unless rescinded or canceled earlier.	

1 PURPOSE

This Departmental Notice (DN) establishes an interim policy for the secure use of wireless network technologies including 802.11, Bluetooth and infrared. While this interim policy meets National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) today, it is subject to revision one year from the date of release as next generation security components become more widely available in the market.

2 POLICY

USDA agencies and staff offices will adopt policies and procedures for 802.11, Bluetooth and infrared technologies that conform to the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) according to the Clinger Cohen Act of 1996.

All wireless networks are required to specifically meet the NIST FIPS requirements for 802.11i technologies found in FIPS 140-2, FIPS 197 and Special Publication 800-38C. Since certified products have not been introduced to the market in sufficient quantity to be easy to acquire and affordable, USDA is adopting a two-stage approach to standards compliance.

- Phase One: For a period of one-year from the date of issue, new systems will be required to meet the minimum specifications introduced in Section 7 of this DN. During this period of transition, it is particularly important for agencies to assess the level of risk associated with investing in Wireless Local and Wide Area Networks (WLANs, WWANs) according to Section 7e. Agencies are responsible for justifying all risks associated with fielding non-CCMP-certified products.
- Phase Two: As NIST-certified equipment is introduced into the market in large enough volumes to make it affordable and easy to acquire, USDA will require agencies to migrate existing networks to a new set of minimum specifications. The contents of this policy are subject to change with the transition to Phase Two.

3 BACKGROUND

US Department of Agriculture (USDA) agencies and staff offices are adopting commercial wireless technologies at a more accelerated pace than in the past, and USDA Departmental Regulations need to more specifically address security risks inherent in those technologies. The Clinger-Cohen Act of 1996 assigns the Secretary of Commerce the responsibility to develop, implement, promulgate, and make compulsory and binding, standards and guidelines pertaining to Federal computer systems through NIST under section 5131 and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

Federal agencies may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer that are more stringent than the standards promulgated by the Secretary of Commerce.

NIST has issued standards for the usage and implementation of cryptography and guidelines for 802.11 and Bluetooth® technologies to deal with vulnerabilities and malicious attacks to Federal systems.

All of the vulnerabilities that exist in a conventional wired network apply to wireless technologies. Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing firewall protections. Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed. Denial of Service attacks may be directed at wireless connections or devices. Malicious entities may steal the identity of legitimate users and use the stolen identities to impersonate them on internal or external corporate networks. Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements. Malicious entities may deploy unauthorized access points to surreptitiously gain access to sensitive information. Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities. Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations. Malicious entities may use third party, untrusted wireless network services to gain access to an agency's or other organization's network resources. Internal attacks may be possible via ad hoc transmissions. [NIST]

"Wireless hackers can download access point software onto an unsecured wireless laptop and masquerade as a legitimate access point." [Defense Information Systems Agency - DISA].

4 APPLICABILITY AND SCOPE

This notice applies to all USDA agency and staff office personnel, including non-government personnel authorized to use USDA wireless networks.

It applies to all commercial wireless devices, services and technologies that transmit voice and data including video. This also includes portable electronic devices (PED) such as laptop computers with wireless capability, cellular/personal communications system (PCS) devices, personal digital assistants (PDA), paging devices, Global Positioning System (GPS) receivers, Radio Frequency Identification Devices (RFID), fixed telemetry devices, and any other commercial wireless devices capable of storing, processing, or transmitting information. Services include Wireless Local Area Network (LAN), Wireless Wide Area Network (WWAN), and Personal Area Network (PAN). This policy does not address classified communications.

5 REFERENCES

National Federal Oversight Guidelines

Committee on National System Security Systems (CNSS). *National Information Assurance (IA) Policy on Wireless Capabilities*, CNSS Secretariat (I01C). National Security Agency. Ft. Meade, Maryland. August 11, 2004

Iorga, Michaela, Gavrila, Serban, Jansen, Wayne, Karygiannis, Tom, Korolev, Vlad. *Policy Expression and Enforcement for Handheld Devices.* National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Federal Register. *Executive Order 13011: Federal Information Technology.* July 16, 1996

Karygiannis, Tom, Owens, Les. *Wireless Network Security, 802.11 Bluetooth® and Handheld Devices.* National Institute of Standards and Technology: Special Publication 800-48.Computer Security Division, Technology Administration, U.S. Department of Commerce. November 2002.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES).* Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce. November 26, 2001.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 140-2:Security Requirements for Cryptographic Modules.* Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce. December 3, 2002.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and*

Information Systems. Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce. December, 2003.

Office of Management and Budget. *OMB Circular A-130, Transmittal Memorandum #4Memorandum for Heads of Executive Departments and Agencies: Management of Federal Information Resources.* November 28, 2000.

US Congress. *Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)) (also known as: Division E: Information Technology Management Reform Act): Section 5002*. United States Code. 1996.

US Congress. *Defense Authorization Act: The Government Information Security Reform Act: Public Law 106-398.* October 30, 2000.

US Congress. *Government Paperwork Elimination Act, 44 USC 3504.* October 21, 2003

Federal Agency Guidelines

Defense Intelligence Agency. *Regulation No. 50-23: Security: DIA Information Systems Security (INFOSEC) Management.* SYS: Defense Intelligence Agency. March 1, 2002

Department of Defense. *802.11 Wireless LAN Security Framework.* Department of Defense: Defense Information Systems Agency Wireless Security Support Program. January 2004.

Assistant Secretary of Defense Networks and Information Integration. *Directive Number 81002.2*, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid (GIG)*. Department of Defense. Washington, DC. April 14, 2004. Retrieved from http://www.dtic.mil/whs/directives/corres/html/81002.htm.

Department of Homeland Security. *Suggested Enhancements: Management Directive 4300A: Policy Directive for Sensitive Systems: Section 2.8 – Designated Accrediting Authority: Section 3.11.5 – Wireless Security Working Groups: Section 4.6 – Wireless Communications: 5th Draft.* Wireless Management Office. May 2004.

Department of Veterans Affairs. *VA Wireless and Handheld Device Security Guideline, Version 2.1.* September 25, 2003.

Defense Information Security Agency. *Wireless Security Technical Implementation Guide, Version 3, Release 1.* DISA Field Security Operations. DISA for DOD. April 15, 2004.

General Services Administration *: CIO 2161.1: Wireless Personal Digital Assistants (PDAs).* General Services Administration. February 6, 2004

USDA Guidelines

Bull, Barre, Cramer, Chuck. *USDA Personal Electronic Device (PED), Security Assessment Guide*. Science Applications International Corporation. September 6, 2001.

Telecommunications Advisory Sub Council. *Technical Recommendations for Wireless Data Network Deployments Within the United States Department of Agriculture.* Strategy Team: Wireless Working Group: Telecommunications Advisory Sub Council. US Department of Agriculture. November 1, 2004.

USDA. *Cyber Security Manual, Series 3500 DRAFT Chapter 10, Information Technology Systems, Part 3, Portable Electronic Devices (PED) and Wireless Technology*. U.S. Department of Agriculture. September 28, 2004.

6 DEFINITIONS

a Access Point. An access point is the entry point from a wireless station to a Wireless Local Area Network (WLAN) or Wireless Wide Area Network (WWAN), from a WLAN or WWAN to a wired Local Area Network (LAN), between WLANs, WLANs and WWANs, or between WWANS. Access points generally consist of a radio, a wired network interface, and management and bridging software. Access point functionality can be implemented using a hardware device or an application installed in another network device (a router for example) and is configured based on architecture requirements. Some vendors have removed the management and bridging software from the access point and placed these features into a wireless switch. In a WLAN system with wireless switches, the access points are usually called access ports and are essentially transceivers (transmitter/receiver of data) with a network interface. Software applications are available that can be used to turn a laptop computer acting as a wireless station (wireless client) into an access point.

b Advanced Encryption Standard (AES): AES specifies a privacy algorithm. It was chosen by the National Institute of Standards and Technology (NIST) to replace NIST standard Data Encryption Standard (DES), and is a Federal Information Processing Standard (FIPS) as defined in FIPS Publication 197. It also meets the NIST FIPS 140-2 specification. It allows administrators to specify key sizes between 128, 192 or 256 bits. Before AES came along cipher techniques encrypted data payloads only. AES encrypts the entire data frame and is much stronger than WEP and TKIP.

c AirCard®: Trademark of Sierra Wireless. Also called a PC Card or Personal Computer Memory Card International Association (PCMCIA) Card. See PCMCIA.

d Bluetooth®: Bluetooth® enabled electronic devices connect and communicate wirelessly via short-range (100m or less) in ad hoc networks called piconets. IEEE 802.15 Wireless Personal Area Networks (WPANs) formalized the specification. The Bluetooth® standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers using short-range connections. Bluetooth® does not address audit and non-

repudiation security services. Since Bluetooth® devices do not register when they join a network, they are invisible to network administrators. Consequently, it is difficult for administrators to apply traditional physical security measures.

e Commercial Wireless: Devices, Services, and Technologies commercially procured and intended for use in commercial and unlicensed frequency bands.

f CCMP: Counter Mode Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP). A data-confidentiality protocol that uses 128-bit encryption. CCMP is an AES standard with a 48-bit IV, and uses AES in a counter mode to achieve confidentiality. It uses an encryption technique called cipher block chaining to perform data integrity checks and authentication. CCMP protects additional parts of the IEEE 802.1X frame known as Additional Authentication Data (AAD). AAD includes the packet source and destinations, and protects against attackers replaying packets to different destinations. CCMP conforms to government standards and offers stronger encryption than TKIP.

g Emergencies: An emergency is any unplanned event that can cause death or significant injury to employees or the public; that can shut down or disrupt operations; or that can cause physical or environmental damage, such as national or declared emergencies, fire emergencies, hazardous materials incidents, storms, communications failure, disaster recovery, and similar emergencies. Note: Failure to plan for a requirement does not constitute an emergency.

h Media Access Control (MAC). A hardware address that uniquely identifies each node of a network. MAC related information in the header of a datagram is sent in a non-encrypted format so it is possible that the MAC address can be obtained by eavesdroppers and spoofed in an attempt to gain access to the WLAN.

i PCMCIA: Personal Computer Memory Card International Association card, also called a PC Card or AirCard®. A PCMCIA card may fit into an open slot in a mobile computing device, or may need to be installed. It can be equipped with a variety of features including modem and network interface capabilities, and may act as a radio transceiver. PCMCIA cards are often configured to work with specific wireless carriers, but may support more than one.

j Peer-to-Peer. WLANs may be configured into a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly. Peer-to-peer WLAN communications can bypass required encryption and authentication mechanisms, making transmissions vulnerable to interception and unauthorized access from outsiders. Peer-to-peer voice communications are an exception to this policy.

k Personal Digital Assistant (PDA). A generic term for a class of small, easily-carried electronic devices used to store and retrieve information.

l Personal Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held laptops computers.

m Piconet: A piconet is established when two or more portable devices make a wireless

connection. When a piconet is formed, one device controls one or more other devices for the duration of the communication session. A piconet is sometimes called a Personal Area Network (PAN).

n Service Set Identifier (SSID). The SSID is an alphanumeric code that corresponds to a specific wireless network (or subsystem). Usually, in the default configuration of an access point, the SSID is transmitted in the clear as a part of a periodic beacon that is sent by the access point, or it may be requested in a probe-request frame when a wireless client attempts to associate with an access point with a specific SSID.

o Spoofing: A technique used to gain unauthorized access to computers, whereby an intruder sends messages to a computer with an Internet Protocol (IP) address masquerading as a legitimate transmission from a trusted host.

p Teleworking: (Also known as flexiplace, flexible workplace, and telecommuting). Performance of official duties at an alternative work site (i.e. home, telecenter, or other satellite work location).

q Vulnerability. Inherent weakness or flaw in a system that if exploited could result in the loss of confidentiality, integrity or availability of an IT resource or data.

r Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use Infrared (IR), acoustic, Radio Frequencies (RF) and optical but, as technology evolves, wireless could include other methods of transmission.

s Wireless Device. Hardware that provides wireless capabilities. This definition includes, but is not limited to wireless handheld devices like PDAs, cellular/PCS phones, two-way pagers; wireless audio/video recording devices; telemetry devices with wireless integrated technologies; electronic tablets and laptop computers.

t Wireless Handheld Device: Small computers often capable of synchronizing with a PC on specific software applications. Many handheld devices are capable of "beaming" data with the use of Infrared (IR) or Bluetooth® technologies. Handheld wireless devices include a range of PDA's and Smart phones, that may combine the capabilities of a traditional PDA, digital cellular telephone with voice services as well as e-mail, text messaging, Web access, voice recognition and any number of applications that serve as productivity tools.

u Wireless Local Area Network (WLAN). WLANs use radio waves for transmission and are generally connected through access points to an existing wired infrastructure, although they may be standalone as well. They provide authorized users access to resources that are not physically connected to their client device. Also known as Wi-Fi or WPA, WLAN communications are governed by the IEEE 802.11 family of standards.

v Wireless Personal Area Network (WPAN). WPANs operate in the Personal Operating Space (POS) of a user, which extends 10 meters in any direction. Also know as Bluetooth®, WPAN communications are governed by the IEEE 802.15 family of standards.

7 PROCEDURES

a Waivers: See Departmental Notice (DN) 3300-14 for information on the acquisition process for wireless products and services and specific waiver requirements. Besides requirements in DN 3300-14, USDA agencies must demonstrate an investment's contribution towards mission results and program performance objectives. As a result, USDA Enterprise Architecture (EA) mapping information must be submitted to OCIO with each waiver request. Agencies are required to map wireless technologies to the USDA EA according to the Office of Management and Budget (OMB)'s Federal Enterprise Architecture (FEA) Business Reference Model (BRM) predefined business lines and sub functions. OMB's BRM numbering scheme shall be associated with each agency's unique Project ID in order to perform the mapping. Technologies that map to OMB's definition of "Services for Citizens" must also map to a "mode of delivery", "line of business" and "subfunction".

In addition, waivers for WWANs and WLANs must include the following information:

(1) Evidence that each network has been certified and accredited for compliance with security requirements (see 7b);

(2) A Return-on-Investment (ROI) analysis (see 7c)

(3) A risk assessment (see 7e)

(4) A block diagram that clearly depicts where the WLAN or WWAN will interface with USDA's enterprise backbone network (UTN), locations of all firewalls and intrusion detection systems.

(5) If the WWAN or WLAN connects to USDA's enterprise backbone network (UTN), agencies and staff offices must conduct a traffic analysis and submit the results with the waiver request that identifies the potential impact on the USDA enterprise backbone network.

b Certification and Accreditation (C&A): Agencies must ensure that USDA owned and operated wireless network systems and their components are certified and accredited according to NIST SP 800-47; OMB Circular A-130; USDA CyberSecurity guidance; and OMB's Circular A-11, Part 7, Section 300.

c Return-on-Investment: Cost benefit and return-on-investment analyses should be prepared according to guidance found in USDA 's Capital Planning and Investment Control Guide and OMB's Circular A-11, Part 7, Section 300.

d Security Categorization: Agencies and staff offices shall categorize standards for wireless technologies according to the Federal Information Processing Standard (FIPS) 199.

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the (OMB) and Congress on the adequacy and effectiveness of information security

policies, procedures, and practices.[NIST]

e Risk Assessments: Risk assessments will be conducted according to the Government Information Security Reform Act and the Clinger Cohen Act prior to the deployment of a wireless network with the following exceptions:

(1) Emergencies: Networks established as the result of an emergency as defined in this Departmental Notice.

(2) Bluetooth®: WPAN networks based on Bluetooth® technologies. Refer to section "f" for Bluetooth® policy.

Risk analyses should be prepared according to guidance found in USDA 's Capital Planning and Investment Control Guide and OMB's Circular A-11, Part 7, Section 300.

f Peer-to-Peer Wireless Networks: Peer-to-peer wireless networks are prohibited with the following exceptions:

(1) Continuity of Operations: Use in continuity of operations (COOP) or emergency response operations. USDA personnel responsible for COOP or emergency response operations must submit an annual approval request to the Associate Chief Information Officer for Telecommunications for an exception to the peer-to-peer restriction. The request must contain:

(a) POC: Requesting Agency/Office/Division/Business Unit or Branch Name and Point-of-Contact;

(b) Description: Number of anticipated users; their titles and organizations; and, a description of the operational need.

(2) Bluetooth® Personal Area Networks: While permitted, the transfer of information using Bluetooth® and infrared technologies are subject to the guidelines found in section 6h of this DN.

g 802.11 technologies: USDA permits the use of Wireless Wide Area Networks (WWAN)s and Wireless Local Area Networks (WLAN)s using 802.11 technologies with the following provisions:

(1) NIST Compliance: All 802.11 networks must fully comply with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 Level 2 Certification as well as the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard. Wi-Fi Alliance certified Wi-Fi solutions must be WPA 2, Advanced Encryption Standards (AES) compliant at a minimum. Component standards shall include:

(a) Advanced Encryption Standards (AES). Note that AES support may require a special gateway or switch for accessing the AES secured network.

(b) Protected Extensible Authentication Protocol (PEAP) or the EAP Tunneled Transport

Layer Security (TTLS): To perform authentication.

(c) 802.1X & RADIUS: 802.1X serving as the port based authentication protocol using a Remote Dial-In User Service (RADIUS) server to perform authentication behind USDA access points.

(d) Virtual Private Network (VPN): The VPN must meet 3DES and Mobile IPSEC standards, and follow users as they roam.

(e) Built-in X.509 certificates: X.509 certificate exchange must be used for secure communication between devices and ensured authenticity to provide for protection of wireless networks against impersonation attacks, whereby a malicious user programs an access point with the same SSID and MAC address as a valid AP in hopes of 'luring' a trusted client.

NIST-approved Equipment: NIST maintains the FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List of all validated FIPS 140-2 cryptographic modules. An alphabetical list of FIPS 140-1 and FIPS 140-2 vendors (vendors with validated cryptographic modules) is also available. Note: Only 140-2 certifications are USDA approved.

Exceptions: Exceptions to the policy may be approved according the following provisions:

Emergencies. If an emergency occurs and the establishment of a wireless network was necessitated by the emergency, agencies or staff offices responsible for the implantation of the 802.11 wireless network shall notify the Associate Chief Information Officer for Telecommunications within 15 days of the initial deployment. Agencies should describe the nature of the incident and the status of the wireless network. The ACIO for Telecommunications will determine whether it is necessary to submit a waiver for continuing operations.

Agencies and staff offices may submit a waiver to request an exception to the provisions specified in this policy based on emergencies, or continuing and compelling business requirements as stated below.

Continuing and Compelling Business Use: Agencies and Staff Offices that believe they have a continuing and compelling business reason for establishing a wireless network non-compliant with USDA guidelines should submit a written request to the ACIO for a waiver. Once submitted, the ACIO shall have 15 days to coordinate with the Associate Chief Information Officer for Cyber Security and respond to the request.

Pre-existing wireless networks: Agencies and Staff Offices with existing 802.11 wireless networks that do not meet the provisions of this Departmental Notice are prohibited from connecting to any other USDA network. Agencies and Staff Offices must upgrade their existing 802.11 wireless networks to meet the provisions of this Departmental Notice within one year after this policy becomes effective.

(2) FISMA Compliance: WLAN/WMAN technologies are subject to the provisions of the Federal Information Security Management Act (FISMA) including the guidance contained in NIST

Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. See Section 6b for C & A guidance.

(3) Configuration Management: Network managers are required to establish and maintain configuration management of all WLAN/WMAN architectures and components and maintain configuration records for periodic inspection by OCIO personnel.

(4) Firewalls: Firewalls are required between wireless networks and wireless to wired infrastructure.

(5) Internet Access: USDA employees may only access the Internet through the authorized USDA network.

(6) Network Monitoring: All wireless networks must include a wireless network-monitoring tool with 802.11 specific diagnostic capabilities and security testing capabilities. Software tools must be integrated into the WLAN/WWAN infrastructure, and be able to perform continuous monitoring and containment of unauthorized wireless configurations, rogue APs, signal leakage, and unauthorized traffic accessing existing authorized configurations. Agencies and Staff Offices must establish procedures to respond to incidents involving unauthorized configurations or intrusions, and signal leakage.

(7) Intrusion Detection: Intrusion detection software must be deployed to analyze AP logs. Solutions shall provide the ability to detect intruders on the network and users will be required to authenticate to the wireless network.

(8) Interference Detection: Radio frequency Interference detection and handling of the interference shall be an inherent part of the wireless network.

(9) Anti-virus Software: Anti-virus software must be maintained on all WLANs/WWANs.

(10) Channel Separation: Network managers are required to maintain a separation of five channels from nearby wireless networks where feasible to prevent interference, according to NIST recommendations.

(11) Access Points (AP)s:

(a) Configuration: Access points shall be configured:

1 With standard, enterprise-wide, system security policies for Virtual Local Area Networks (VLAN)s, security, and Quality of Service (QoS).

2 To uniformly enforce security, quality of service, and user policies for varying classes of devices, including handheld scanners, PDAs, and notebook computers.

3 With interfaces that encompass all layers of a wireless network, including the radio, MAC, and network layers.

4 In a manner that does not pose a significant risk if stolen or compromised.

5 To permit only APs with proper certificates the ability to communicate with one another in order to immediately detect a device impersonating an AP.

(b) Registration: Access points will be registered with the associated Agency or Staff Office and should be reported to the Department on a regular basis. (See DN 3300-15 on Wireless Asset Management)

(c) Recordkeeping: Access points must maintain record logs on non-authorized access attempts for a minimum of thirty days. Recording capabilities must be active at all times while access points are operational.

(d) Location: AP's will be located on interior walls of buildings. AP locations near or on exterior walls or outside windows are prohibited.

(12) Service Set Identifiers (SSIDs): Methods for connections are SSIDs. SSID character strings will not reflect the name of the Department, Agencies or Staff Offices, offices addresses or other identification information. OCIO shall develop a USDA-wide naming convention and tracking mechanism for SSID character strings. Agencies and staff offices will utilize the OCIO established naming convention when creating SSIDs and submit them to National Telecommunications Services and Operations (NTSO) for approval before use. Guest connections should be logically redirected to broadcast SSIDs located at the network perimeter where guests can pass through the same security controls that are applied to external connections.

(13) Antennae: Direction antennas should be installed where possible to limit unauthorized access USDA network.

(14) WLAN/WWAN Clients: Client devices must interface to USDA WWLANs/WWANs in the following manner:

(a) Permission for Access: Network access will only be granted to clients that request authentication to network resources via 802.1X transport and a Virtual Private Network (VPN).

(b) AES Compliance: Registered clients that interface with WLANs and WWANs must be AES compliant, configured to ensure maximum security, and purchased to support firmware upgrades so that security patches may be deployed as they become available. The use of a special gateway or switch is permitted for devices not equipped to support AES.

(c) Wired Connections: WI-Fi functionality on laptops or PDAs will be disabled when connected to a wired network.

(d) File Sharing: File sharing will be disabled on wireless laptops and handheld devices.

(e) Software: Registered clients must actively utilize and update anti-virus, anti-spyware, and personal firewall software. Agencies and Staff Offices must regularly install up-to- date security patches on registered clients. Agency administrators should ensure that client

software tools will interoperate effectively with existing WLAN/WWAN network software prior to purchase.

(15) Audits: Audits will be conducted by Cyber Security to ensure that WLAN and WWAN technologies are properly configured from end-to-end. Audits will include use of tools to examine airborne packets for threats involving Internet Protocol (IP) spoofing in addition to tools for other types of monitoring. Cyber Security will record the results of their findings and submit a report to the Associate CIO for Telecommunications upon completion.

(16) Expertise: Agencies deploying 802.11 technologies are required to identify and train a technical or telecommunications specialist according to DN 3300-16 to implement, and ensure agency compliance with the 802.11 provisions in this directive. Agencies and Staff offices must submit the following information to the Associate Chief Information Officer for Telecommunications for each WLAN/WWAN they operate, or for each WLAN/WWAN operated by a third party on their behalf:

(a) The location(s) of each WLAN/WWAN

(b) The locations of all Access Point (AP)s.

(c) The name, telephone number and email address for each WLAN/WWAN point-of-contact.

(17) Expert Training: Agencies and Staff Offices are required to provide biannual training on configuration management and current standards requirements for Technical Specialists and Managers overseeing the technical planning, design, implementation, operations or maintenance of WLAN/WMAN technologies. Training will be conducted according to the provisions of DN 3300-16.

(18) User Training: Annual security awareness training must be conducted for all WLAN/WMAN users. Agencies and staff offices may want to consider conducting wireless network security awareness training for all employees.

(19) Equipment disposal: Agencies and Staff Offices must use Federally-approved applications or processes for eliminating USDA information from wireless hardware or equipment (e.g. access points, switches, etc.) when disposing of excess property.

(20) Teleworking: The use of Wireless Wide Area Networks (WWAN)s and Wireless Local Area Networks (WLAN) technologies for teleworking must be approved by a USDA Cyber Security representative or Agency Information Systems Security Program Manager (ISSPM), who has conducted an on-site inspection for compliance with USDA and other Federal guidelines. The ISSPM or Cyber Security representative will verify the use of a Secure Socket Layer (SSL) protocol, Virtual Private Network (VPN), or 802.11i with AES in the CCMP mode.

(21) Moves, Adds & Changes: Agencies and Staff Offices must comply with USDA policy for moves, adds and changes as outlined in DN 3300-15.

h Bluetooth® or Infrared technologies:

(1) Transmission Guidelines: Bluetooth® or infrared transmissions are restricted to the transfer of data between two government-owned devices for purposes such as:

(a) Synchronizing between a government-owned PDA and a government-owned laptop;

(b) Exchanging contact information between two federal employees' PDAs; or

(c) Personal Area Network (PAN) transmissions within the confines of a secure government facility.

(2) Expertise: Agencies deploying Bluetooth® or infrared technologies are required to identify and train a Bluetooth®/infrared administrator to implement and ensure agency compliance with the Bluetooth® provisions in this directive.

(3) Encryption: All Bluetooth® traffic must be encrypted according to the Bluetooth® specification for Encryption Mode 3; and access services are required to comply with Service Level 1.

(4) Authentication: Agencies are required to install application-level password authentication software to secure each Bluetooth® or infrared device. Agency administrators must ensure device mutual authentication for all accesses.

(5) Personal Identification Numbers (PIN)s: Bluetooth® PINs must conform to the password policy found in DN # 3300-13 on Wireless Devices. Administrators must configure Bluetooth® devices to delete PINs after initialization to ensure that PIN entry is required every time, and that the PINs are not stored in memory. Agencies shall use an alternative protocol to the default for the exchange of PIN codes, such as certificate-based encryption key exchange methods at the application layer.

(6) Key Size: All Bluetooth® or infrared applications are required to set the encryption key size parameter at a minimum accepted length of 64 bits, and administrators are encouraged to set the minimum key size parameter to full 128 bits. Agencies should ensure that combination keys are used instead of unit keys. Agencies are encouraged to use smart card technology for key management.

(7) Sensitive Applications: Agencies are required to use application-level encryption and authentication (on top of the Bluetooth® or infrared stack), for highly sensitive data communication.

(8) Facility Guidelines: Agencies are required to maintain a secure perimeter such that on-site network users can maintain secure connections in their office spaces. Power settings should be low enough to prevent outsiders from detecting devices in operation on the agency's premises.

(9) Deactivating transmission functionality: Agencies must require users to turn off the Bluetooth® or infrared function on wireless devices at all times when not in use.

(10) Antivirus: Bluetooth® enabled hosts are required to have antivirus software installed.

(11) Software patch updates: Agencies are required to regularly test and deploy Bluetooth® software patches and upgrades.

(12) Intrusion Detection: Agencies are encouraged to deploy intrusion detection agents on the network that can detect suspicious behavior or unauthorized access and activity, and deactivate rogue Bluetooth® or infrared devices.

8 INQUIRIES

Direct all questions concerning this notice to the Telecommunication Policy and Planning Division, Telecommunications Services and Operations, Office of the Chief Information Officer.